UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, Plaintiff, v. BRENDAN JOHNSTON, Defendant.	14-CR-404-JMF

DEFENDANT BRENDAN JOHNSTON'S RESPONSE TO THE GOVERNMENT'S SENTENCING MEMORANDUM

June 15, 2015

Michael Zweiback
Admitted Pro Hac Vice
Arent Fox LLP
555 West Fifth Street, 48th Floor
Los Angeles, CA 90013-1065
213.629.7400

Attorneys for Defendant
Brendan Johnston

Arent Fox

Arent Fox LLP / Attorneys at Law
Los Angeles, CA / New York, NY / San Francisco, CA / Washington, DC
www.arentfox.com

June 15, 2015

Michael Zweiback
Partner
213.443.7651 DIRECT
213.629.7401 FAX
michael.zweiback@arentfox.com

VIA E-MAIL

The Honorable Jesse M. Furman
United States District Judge
Southern District of New York
Thurgood Marshall United States Courthouse
40 Centre Street, Room 2202
New York, NY 10007

Re: United States v. Brendan Johnston, Case No. 14-CR-404

Dear Judge Furman:

In the course of summarily dismissing the mitigating impact of Mr. Johnston's [redacted] (*see* Government's Sentencing Memorandum ("Gov. Mem.") 9), the government notes that the other three Blackshades defendants who have been sentenced each also sought leniency based on mental health issues. But, the government fails to explain that, as to two of those defendants, the government granted leniency by permitting them to plead to lesser charges.

Marlen Rappa was a 42-year-old man who infected almost 100 computers and used victims' webcams to take screen shots of the victims naked and having sex. (*See* Gov. Mem. 7.) He was originally charged with 18 U.S.C. § 1030(a)(5)(A), the same offense to which the government required Mr. Johnston to plead guilty. However, the government allowed Mr. Rappa to plead guilty to a [redacted] (Rappa Sentencing Transcript ("Sent. Tr.") 13:9-12, 35:13-17 (attached as Ex. 1).) The government's decision reduced Mr. Rappa's advisory Guidelines range by at least four levels. (*See* U.S.S.G. § 2B1.1(b)(18)(ii).)

Juan Sanchez, who used the Blackshades keylogger on approximately 90 computers and downloaded files from seven computers (*see* Rappa Gov. Mem. 4 (attached as Ex. 2)), received an even greater benefit based, at least in part, on his mental health. The government allowed Mr. Sanchez to plead guilty to a misdemeanor and he was sentenced to one year of probation. At sentencing, the court and government explained the significance of Mr. Sanchez's mental health history. (*Id.*) The government noted that Mr. Sanchez sought mental health treatment before his arrest. (*Id.*) The court noted that Mr. Sanchez's computer hacking did not appear to be malicious and appeared to result from computer addiction, which was related to his other mental and emotional issues. (*Id.*) [redacted] (PSR ¶ 80.)

Mr. Johnston believes that the government is incorrect when it concludes that a within-Guidelines sentence is appropriate. Mr. Johnston's documented [redacted] supports a significant variance from the Guidelines range, particularly when considered in light of his other background and characteristics. *See Gall v. United States*, 552 U.S. 38, 56-59 (2007) (upholding sentence of probation where Guidelines range was 30-37 months based on defendant's voluntary withdrawal from conspiracy, defendant's post-offense conduct and rehabilitation, support from defendant's family and friends, defendant's lack of criminal history, and defendant's age (21) at the time of the offense). The Probation Officer agreed. (PSR 25-26.)

The government claims that incarceration is necessary to avoid unwarranted sentencing disparity between Mr. Johnston, Mr. Rappa, and Mr. Fedorek. (Gov. Mem. 9.) The government fails to note, however, that it has described Mr. Fedorek as a "resourceful and determined hacker." (Fedorek Gov. Mem. (attached as Ex. 3).) Mr. Fedorek infected over 400 computers, possessed over 50,000 stolen credit card numbers, and had numerous forms of malware on his computer including files for creating counterfeit websites for American Express, Bank of America, and PayPal. (*Id.*) Moreover, Mr. Fedorek was in criminal history category II. At the time of sentencing, Mr. Fedorek also had a felony drug charge that was pending in state court and he requested the 24-month sentence that was imposed so that he could serve his entire anticipated state sentence in federal custody. (*See* Fedorek Sent. Tr. 14:15-24, 25:20-22 (attached as Ex. 4).) In support of its recommendation of a 6-12 month sentence for Mr. Rappa, the government explained, "Indeed, it is difficult to imagine a more serious violation of a computer user's privacy than that committed by [Mr. Rappa] over and over again. . . ." (Ex. 2 at 4-5.)

The government's attempt to equate Mr. Johnston to Mr. Rappa and Mr. Fedorek are unavailing. Mr. Johnston was not involved in using the Blackshades tools maliciously. He did not hack into victims' computers and did not steal anything or invade anyone's privacy. Moreover, he has no criminal history. Thus, the sentences imposed upon the other defendants support Mr. Johnston's requested sentence of probation.

The government repeatedly cites the goal of general deterrence to support its argument for a within-Guidelines sentence. (*See* Gov. Mem. 8, 9.) But, as explained above, there is wide disparity in the government's treatment of and sentences imposed upon the actual users who maliciously infected other computers to steal personal and financial information, hijack webcams, and spy on people in their most intimate moments. Three such defendants received sentences ranging from misdemeanor probation up to 24 months imprisonment. The disparate treatment of these defendants undermines the government's emphasis on general deterrence.

The government also claims there is substantial reason to doubt Mr. Johnston's statement of the offense. (Gov. Mem. 8.) Preliminarily, we note that Mr. Johnston's statements regarding his offense conduct have been consistent throughout this litigation. His sentencing memorandum contains the same statement of his offense conduct that he offered at his change of plea hearing (Change of Plea Tr. 20:7-24, 22:1-7 (attached as Ex. 5).) and in the PSR. (PSR ¶ 46.) The government did not object to either of those statements.

The government appears to have misunderstood Mr. Johnston's sentencing memorandum, which possibly explains the government's response. The government incorrectly states that Mr. Johnston claims he continued selling the RAT for only about 45 days after he realized the "illicit" nature of the RAT. (Gov. Mem. 8.) But, that is not what Mr. Johnston said.

To clarify, Mr. Johnston acknowledged that, after he started working for Blackshades, he learned that some customers were using the products for illicit purposes. (Def. Mem. 9.) The reference to "45 days" relates specifically to the time when Mr. Johnston learned how Marjinz was using the "backdoor" feature on the RAT to gain access to all computers onto which the RATs were installed. The defense believes that point in time is relevant because, at that point, Mr. Johnston knew that he was aiding Marjinz in illegal activity by marketing and selling the RAT. Prior to that, Mr. Johnston was aware of what users could do with the RAT and we did not mean to imply otherwise in the sentencing memorandum.

In arguing that Mr. Johnston was in a position to understand the damage that the RAT could cause, the government selectively quotes from Mr. Johnston's [redacted] (Gov. Mem. 8.) But, the government failed to mention other key statements [redacted] including: Mr. Johnston never had access to the Blackshades server; Mr. Johnston had no interest in using the Blackshades tool; some people, including the CEO of Paypro, used Blackshades to monitor their kids; after leaving Blackshades, Mr. Johnston worked on anti-malware projects; and after leaving Blackshades, Mr. Johnston offered a person who hosted a website money not to host Blackshades.

Mr. Johnston has been consistent throughout this case regarding his knowledge of and participation in Blackshades. He has and continues to fully accept responsibility for his actions.

Respectfully submitted,

Michael Zweiback

Michael Zweiback

Attachments (Exhibits 1-5)

cc: Daniel Noble (w/ Attachments)
Sarah Lai (w/ Attachments)

EXHIBIT 1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

UNITED STATES OF AMERICA, New York, N.Y.

v. 14 Cr. 0544(VEC)

MARLEN RAPPA,

Defendant.

----------x

April 22, 2015
2:00 p.m.

Before:

HON. VALERIE E. CAPRONI,

District Judge

APPEARANCES

PREET BHARARA
United States Attorney for the
Southern District of New York
BY: DANIEL S. NOBLE
Assistant United States Attorney

COLSON & HARRIS LLP
Attorneys for Defendant
BY: JUSTINE A. HARRIS

- also present -

SA Samad Shahrani, FBI

SA Patrick Hoffman, FBI

past, I apologize -- Mr. Rappa's offense conduct was symptomatic, was interconnected, linked very closely with serious mental health problems, that it really was a way to treat -- it was both a symptom of his mental health problems and it was a way almost that he sought, in a poor and terrible fashion, but to self-medicate. And I don't mean that sort of blithely and I don't mean -- it oversimplifies it but it is very much connected to his mental health problems.

And your Honor obviously has read the psychiatric evaluation, but it really sets out a long history, preceding the offense conduct by many, many years, of severe and deep anxiety, depression, panic attacks. And Dr. Bardey did diagnose Mr. Rappa as suffering from severe depressive disorder with prominent anxiety. It was obviously compounded by marital problems, social isolation, a long period of unemployment, and as a result, in sort of layman's terms, that he really was -- his thoughts, his mood -- he was plagued by thoughts of worthlessness, hopelessness, incredibly low self-esteem, and all of these, the sort of factors, converge together, in essence, so that he did turn to the Internet and to escape. These are Dr. Bardey's words, "to escape from these ongoing feelings of depression and worthlessness." He lost himself on the Internet and that was a way to serve as a distraction, as a diversion from his depression and invisible life, and it was in that context that he came upon Blackshades.

happen again. I know that maybe many defendants say that but I know in my heart that I will never be in this situation again, and I need to say this to your Honor and my family and the community.

Thank you.

THE COURT: Thank you, Mr. Rappa.

Mr. Noble, would you like to be heard?

MR. NOBLE: Judge, perhaps just briefly.

A lot has been said and the government appreciates Mr. Rappa's statements and arguments made on his behalf. But Mr. Rappa hit on something that is kind of the white elephant that's in the room or not in the room, and that's the victims here. And, you know, there are mitigating circumstances in this case; the government recognizes that. That's one of the reasons why the government entered into the plea agreement that it did and allowed the defendant to plead to a lesser charge than some of the other defendants in this case.

But Mr. Rappa's personal issues don't diminish the seriousness of the crime that was committed. You know, what we're facing here in these types of cybercrimes is really the democratization of cyberhacking. Mr. Rappa is not a hacker but he was somebody who for $45 could purchase a tool and use it to spy on approximately 90 victims, to record people in their most intimate moments. And that conduct must be punished. A message must be sent to the public that that type of conduct

EXHIBIT 2

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

April 6, 2015

BY ELECTRONIC MAIL

The Honorable Valerie E. Caproni
United States District Judge
Southern District of New York
Thurgood Marshall United States Courthouse
40 Foley Square
New York, New York 10007

Re: United States v. Marlen Rappa,
14 Cr. 544 (VEC)

Dear Judge Caproni:

The Government respectfully writes in advance of the sentencing scheduled in the above-referenced case for April 13, 2015, and in response to the defendant's supplemental sentencing memorandum dated April 1, 2015 ("Def. Supp. Mem.").

At the proceeding on March 13, 2015, the Court indicated that it saw "clear grounds for an upward departure," pursuant to Application Note 20(A)(ii) to Section 2B1.1 of the United States Sentencing Guidelines ("Guidelines" or "U.S.S.G."), based on the substantial invasions of privacy in this case. (3/13/15 Sent. Tr. 4). As the Government noted at the March 13 proceeding, the stipulated Guidelines range in the parties' plea agreement did not include the upward departure now contemplated by the Court. Accordingly, the Government does not advocate for such a departure in this case. Nevertheless, the Government submits this letter to address some of the issues raised in the defendant's supplemental submission.

The defendant urges the Court not to upwardly depart under Application Note 20(A)(ii), or vary upward under 18 U.S.C. § 3553(a), on the grounds that the Guidelines already account for the defendant's invasion of his victims' privacy through (1) the two-level enhancement for a Section 1030 offense involving "intent to obtain personal information," *see* U.S.S.G. § 2B1.1(b)(17)(A); and (2) the four-level enhancement because there were between 50 and 250 victims, *see id.* § 2B1.1(b)(2)(B). (Def. Supp. Mem. 2-6). Application of these two

enhancements under U.S.S.G. § 2B1.1, however, does not necessarily preclude an upward departure under Application Note 20(A)(ii).[1] While it is true that the Sentencing Commission added the two-level enhancement under § 2B1.1(b)(17)(A) specifically "to account for harm resulting from computer offenses that compromise personal information," U.S. Sentencing Comm'n, *Report to the Congress: Increased Penalties for Cyber Security Offenses* (May 2003) ("May 2003 Report") at 11, the Sentencing Commission did not simultaneously "narrow[] the scope of Application Note 20," as the defendant asserts. (Def. Supp. Mem. 4). The defendant points to language added by the Sentencing Commission to Application Note 20 stating that an upward departure is warranted for a Section 1030 offense where "death resulted." The Sentencing Commission made clear, however, that the addition of this language was intended to "*expand[]* the upward departure provision in § 2B1.1 addressing substantial non-monetary harms to account for violations of 18 U.S.C. § 1030 that result in death." (May 2003 Report at 5 (emphasis added)). Moreover, the Sentencing Commission reiterated that the "list of factors a court may consider in determining whether an upward departure would be warranted" in Application Note 20 was "non-exhaustive." (*Id.*). Thus, the Sentencing Commission's addition of the two-level enhancement under § 2B1.1(b)(17)(A) simply did not work to preclude the availability of an upward departure under Application Note 20 in cases involving "a substantial invasion of a privacy interest." U.S.S.G. § 2B1.1, cmt. n. 20(A)(ii) (2014). Likewise, application of the victim enhancement under § 2B1.1(b)(2)(B) does not limit the availability of an upward departure under Application Note 20(A)(ii).[2] While this enhancement captures, to a

---

[1] The Government does not understand the defendant to argue that application of the victim and "personal information" enhancements under § 2B1.1 in any way prevents the Court from considering an upward variance under Section 3553(a).

[2] Although the defendant stipulated in the plea agreement to a four-level enhancement based on the number of victims, he now questions the "technical" applicability of that enhancement because "there was no 'actual loss determined under subsection (b)(1).'" (Def. Supp. Mem. 5). The Government disagrees. As an initial matter, the "court is not required to calculate the amount of loss with certainty or precision but 'need only make a reasonable estimate of the loss' that is 'based on available information.'" *United States* v. *Norman*, 776 F.3d 67, 79 (2d Cir. 2015) (quoting U.S.S.G. § 2B1.1 cmt. n.3(C)). Here, the trove of data that the defendant stole from his victims' compromised computers, including pornography that victims obtained on the Internet, had at least some nominal market value. *See* U.S.S.G. § 2B1.1, cmt. n.3(C)(i) (stating that in calculating loss, the court should consider the "fair market value of the property unlawfully taken, *copied*, or destroyed" (emphasis added)). Further, it is undisputed that installation of the Blackshades malware compromised the integrity of victims' computers, thus necessitating at least some remedial measures that would have imposed losses on victims in terms of repair costs and/or lost computer system time. *See* U.S.S.G. § 2B1.1, cmt. n.3(A)(v)(III). Accordingly, even if the victim's nominal losses combined did not exceed the $5,000 threshold so as to trigger a loss enhancement under § 2B1.1(b)(1), the actual pecuniary losses to the victims nevertheless qualify them to be counted under § 2B1.1(b)(2). In any event, the defendant does not challenge the application of the victim enhancement in this case,

certain extent, the scope of the defendant's offense based on the numerical quantity of victims, it certainly does not account for the nature and severity of the harm that each victim suffered. Thus, while the Government is not advocating for an upward departure pursuant to Application Note 20, such a departure could be applied by the Court based on substantial non-monetary harm under the Guidelines notwithstanding the other enhancements to which the parties stipulated in the plea agreement. Moreover, the Court can and should consider the defendant's egregious and repeated invasions of his victims' privacy in its assessment of the factors set forth in 18 U.S.C. § 3553(a), particularly the nature, circumstances, and seriousness of the offense.

In urging leniency under 18 U.S.C. § 3553(a), the defendant also argues that his case more resembles that of Juan Sanchez, a Blackshades customer who pled guilty to a misdemeanor Section 1030(a)(2)(C) offense and was sentenced to one year of probation, than that of Kyle Fedorek, a Blackshades customer who stole victims' financial account user credentials and was sentenced to 24 months' imprisonment. To be sure, there are differences between the defendant's and Fedorek's cases, including that: (1) Fedorek pled guilty to a Section 1030(a)(5)(A) offense, which triggered a four-level enhancement, *see* U.S.S.G. § 2B1.1(b)(18)(A)(ii), that does not apply here; (2) Fedorek infected over 400 victims' computers, from which he obtained approximately 90 unauthorized access devices (in the form of financial account user credentials), resulting in a "loss" under § 2B1.1 of $45,000; and (3) Fedorek was in Criminal History Category II based on two earlier DWI convictions, and had been charged and intended to plead guilty to a marijuana trafficking offense in New Jersey.

The defendant fails to acknowledge, however, the substantial similarity in the core harm caused his and Fedorek's computer hacking – namely, invasion of privacy – which was the primary driver of Fedorek's sentence. Indeed, in sentencing Fedorek to a below-Guidelines term of 24 months' imprisonment, Judge Vernon S. Broderick discounted the financial aspects of Fedorek's crime (*see, e.g.*, Fedorek Tr. 34-35 (stating that the Guidelines calculation "overstates the seriousness of the offense" given that "there is no evidence that Mr. Fedorek used any device and there's no evidence that there was an actual financial loss by any of the victims")), and instead emphasized Fedorek's invasion of his victims' privacy (*see id.* at 34 ("There's still no escaping that the defendant stole and invaded the privacy of his victims. In many ways, computers have replaced photo albums, phone directories, and diaries . . . . So, in many ways, it was as if the defendant literally entered the homes of these victims and stole their valuables."). Furthermore, Judge Broderick's sentence took into account Fedorek's mitigating mental health circumstances, including depression, which resemble those cited by the defendant in urging leniency here. (*See id.* at 31 ("I do believe that Mr. Fedorek's health issues that began when he was age 16, combined with the apparent impact those issues had on him, warrant consideration as part of his sentence.")).

---

affirming that he "abides by the terms of the plea agreement and the stipulation of the Guidelines range." (Def. Supp. Mem. 6 n.2).

Moreover, the circumstances of the defendant's offense and mental health issues are easily distinguishable from those of Sanchez. A search of Sanchez's computer revealed that he had attempted to use the Blackshades keylogger on approximately 90 computers – mostly to obtain random information rather than specific user credentials, like Fedorek – which triggered a four-level victim enhancement under § 2B1.1(b)(2)(B). Yet it appeared that Sanchez had downloaded files, including photographs, from only seven victims' computers – substantially fewer than in this case. Further, the initial and primary target of Sanchez's hacking attempts was his ex-girlfriend, who told the agents that she was not particularly disturbed by the intrusion under the circumstances. Sanchez also suffered from more extreme and long-lasting mental health issues and, unlike the defendant, had actually sought mental health treatment over one year *prior* to his arrest for using Blackshades. Indeed, at sentencing, Magistrate Judge James C. Francis IV commented that Sanchez's case was "a unique one," and that the offense "appears to have been a consequence of computer addiction, . . . which was itself symptomatic of the defendant's other mental and emotional issues, and certainly, it does not appear that the hacking involved here was malicious." (Sanchez Tr. 6). Accordingly, the defendant's attempt to equate his case to that of Sanchez, rather than Fedorek, is unavailing.

The defendant argues that this case is distinguishable from those where sentences exceeding one year of imprisonment were imposed based on the perceived need to protect the public from the defendants, *see, e.g.*, *United States* v. *Reithmeyer*, 426 F. Supp. 2d 893 (E.D. Ark. 2006); *United States* v. *Hugh*, 533 F.3d 910 (8th Cir. 2008), and cases involving violations of New York State's unlawful surveillance law where indeterminate sentences of one to three years' imprisonment were imposed, *see, e.g.*, *People* v. *Piznarski*, 113 A.D.3d 166 (3d Dep't 2013); *People* v. *Stearns*, 39 A.D.3d 973 (3d Dep't 2007); *People* v. *Church*, 31 A.D.3d 892 (3d Dep't 2006); *People* v. *Evans*, 27 A.D.3d 905 (3rd Dep't 2006). (Def. Supp. Mem. 13-16). To be sure, in light of the history and characteristics of the defendant, the need for specific deterrence in this case is not as substantial a factor as in *Reithmeyer* or *Hugh*. But the need for general deterrence to prevent others from committing similar computer hacking offenses is stronger here than in those cases, which involved more aberrational, even bizarre, conduct by the defendants that others were unlikely to repeat. Furthermore, while some of the state unlawful surveillance cases involved aggravating circumstances, such as the abuse of positions of trust or previous similar conduct by the defendants, these factors do not substantially differentiate the core harm – namely, invasion of privacy – caused by the defendants in those cases from that of the defendant here.[3] Indeed, the defendant's conduct in this case, particularly his manipulation of numerous victims' webcams to photograph them while disrobed or engaged in sexual acts, was in many ways *more* egregious than the defendants' conduct in those cases, all of which involved ten or fewer victims. Thus, a sentence within the applicable Guidelines range of 6 to 12 months' imprisonment in this case certainly would not create an unwarranted sentencing disparity with the cases that the defendant attempts to distinguish.

---

[3] The Government acknowledges, of course, that unlike in *Piznarski*¸ there is no evidence that the defendant used any of the material he stole from his victims to harass or extort them.

Finally, to the extent the defendant argues for a sentence of probation because he is a first-time offender who did not commit a "serious crime" (Def. Supp. Mem. at 19-20), he is plainly mistaken. Although the defendant states that he "deeply regrets his actions, is ashamed and full of remorse" (*Id.* at 18), his failure to acknowledge the extremely serious nature of his computer-hacking offense is troubling. Indeed, it is difficult to imagine a more serious violation of a computer user's privacy than that committed by the defendant over and over again in this case. A substantial sentence that sufficiently reflects the seriousness of this harm is, therefore, clearly warranted.

For the foregoing reasons, and the reasons set forth in our initial sentencing submission, the Government respectfully submits that the defendant's egregious and repeated invasions of his victims' privacy, when considered in conjunction with all of the factors under 18 U.S.C. § 3553(a), supports the imposition of a Guidelines sentence in this case.

Respectfully submitted,

PREET BHARARA
United States Attorney

By: 

Daniel S. Noble
Assistant United States Attorney
(212) 637-2239

Enclosures

cc: Justine Harris, Esq. (via electronic mail)
Attorney for Marlen Rappa

EXHIBIT 3

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	14 Cr. 548 (VSB)
KYLE FEDOREK, a/k/a "kbello," a/k/a "kbella,"	:	
Defendant.	:	

GOVERNMENT'S SENTENCING MEMORANDUM

PREET BHARARA
United States Attorney for the
Southern District of New York,
Attorney for the United States of America.

SARAH Y. LAI / DANIEL S. NOBLE
Assistant United States Attorneys
– Of Counsel –

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

February 17, 2015

BY ECF AND EMAIL

Hon. Vernon S. Broderick
United States District Judge
Southern District of New York
40 Foley Square
New York, NY 10007

Re: *United States v. Kyle Fedorek*
14 Cr. 548 (VSB)

Dear Judge Broderick,

Sentencing in the above-referenced matter is scheduled for February 19, 2015, at 10:00 a.m. The Government respectfully submits this letter in advance of sentencing for the Court's consideration.

The United States Probation Office has calculated a United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") range of 41 to 51 months' imprisonment, as set forth in their Presentence Investigation Report ("PSR"). The Government respectfully submits that a sentence within that Guidelines range is sufficient, but not more than necessary, to provide just punishment, promote respect for the law, and provide deterrence for a serious offense that involved infecting over 400 victims' computers with malicious software, or malware, known as the Blackshades Remote Access Tool ("RAT"). Defendant Kyle Fedorek ("Fedorek" or the "defendant") used the RAT primarily to steal victims' usernames and passwords for various financial, email and social networking accounts.

As discussed in the PSR, Fedorek was a customer of the Blackshades organization. He purchased the Blackshades RAT in or about September 12, 2012. (PSR ¶ 34(a)). Based on an analysis of Fedorek's laptop computer, which was seized pursuant to a search warrant at the time of his arrest, the last time that he downloaded stolen data from any victim's computer was in November 2013. The feature of the RAT that Fedorek used the most was a feature known as "form grabber." This feature was configured to search for financial account information, deployed on over 400 victim computers (PSR ¶ 36(a)), and used successfully to steal financial account log-in credentials from approximately 90 of those computers. In addition, Fedorek used the RAT to steal usernames and passwords for victims' email and social media accounts. The Government has not been able to determine from the analysis of the laptop whether Fedorek used the stolen log-in credentials. While some of the accounts associated with the stolen usernames

and passwords had experienced fraud, the financial institutions where the accounts were held were unable definitively to attribute the fraud to any particular malware.

The analysis of Fedorek's laptop showed that in addition to data stolen using the Blackshades RAT, he also possessed data stolen through other means and other types of malware. Although not part of the charged offense, Fedorek's possession of other malware is relevant to the nature and characteristics of the defendant. For example, Fedorek's laptop stored a database of 50,000 credit card numbers with corresponding expiration dates and security codes. (PSR ¶ 36(d)). The file name of this database suggested that the credit card information was stolen by a hacking group.

In addition, Fedorek's laptop also contained other malware, including, among others:

- at least two other types of keyloggers, besides the Blackshades keylogger;
- executable files for at least two known banking Trojans, *i.e.*, malware designed to steal bank account log-in credentials;
- a program which sends spam to instant messaging services such as ICQ and AOL Instant Messenger;
- an executable file for malware used to launch Distributed Denial of Service ("DDoS") attacks;
- two cryptors, *i.e.*, malware which is used to obfuscate viruses to prevent their elimination by antivirus software;
- four penetration testing tools which are designed to find and exploit security vulnerabilities on webpages, a common method of compromising websites;
- files for creating counterfeit websites for American Express, Bank of America and PayPal; such fake websites are often used by cyber criminals to deceive victims into divulging their account access and personal identification information; and
- proxy programs, which are software programs that obfuscates the user's true Internet Protocol address, and hence, physical location.

(PSR ¶ 36).

The information stored in Fedorek's laptop was extensive and carefully organized. The level of organization, together with the variety of malware stored on Fedorek's computer, suggests that he was a resourceful and determined hacker. While the Government is sympathetic to Fedorek's medical condition, it cannot excuse his criminal conduct.

The defendant contends that a sentence within the Stipulated Guidelines Range of 41 to 51 months would overstate the seriousness of the offense because the Guidelines for computer

hacking "are a poor gauge for evaluating behavior such as that exhibited by Mr. Fedorek in this case." (Def. Ltr at 11). The Government disagrees. The enhancement based on the loss amount – calculated by multiplying the number of stolen access devices (here, usernames and corresponding passwords are counted as one device) by $500 per access device, *see* U.S.S.G. § 2B1.1 comment n. 3(F)(i) (loss "shall be not less than $500 per access device") – is actually a *conservative* estimate. As discussed above, the defendant possessed some fifty *thousand* credit card numbers together with their expiration dates and security codes. However, because it is unclear how and when Fedorek obtained that database, we did not include that database as relevant conduct to which the $500 per access device formula would otherwise apply.

The other enhancements in the Guidelines calculation do not substantially overlap with each other or with the enhancement based on the loss amount. Each enhancement focuses on an aspect of the defendant's conduct that is not necessarily present in every computer hacking scheme. Thus, it is because Fedorek used the Blackshades RAT to steal usernames and passwords for both email accounts as well as financial accounts that he received the additional enhancement for stealing personal information under U.S.S.G. § 2B1.1(b)(17). Similarly, it is because he indiscriminately infected the computers of over 400 victims that he received the enhancement under U.S.S.G. § 2B1.1(b)(2)(C). And because Fedorek intended to, and did, undermine the integrity of his victims' computers, the four-level enhancement under U.S.S.G. § 2B1.1(b)(18)(A)(ii) must be applied. Each of these enhancements reflects specific harm caused by the defendant's offense conduct.

In addition to the seriousness of the offense and the nature and characteristics of the defendant, the need for general deterrence requires a Guidelines sentence. Computer hacking is becoming an ever increasing threat. Given the anonymity of the Internet and the proliferation of tools available to cyber criminals to evade law enforcement (*e.g.,* tools like the cryptors and proxy programs which Fedorek possessed), a sentence within the Stipulated Guidelines Range of 41 to 51 months is necessary to deter others from engaging in cybercrime.

CONCLUSION

For the reasons discussed above, the Government respectfully submits that a sentence within the Stipulated Guidelines Range of 41 to 51 months should be imposed.

Respectfully yours,

PREET BHARARA
United States Attorney

By: /Sarah Y. Lai/
Sarah Y. Lai / Daniel S. Noble
Assistant United States Attorneys
(212) 637-1944 / 2239

cc: Maurice Sercarz, Esq. (by ECF)

EXHIBIT 4

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

UNITED STATES OF AMERICA,

v. 14 CR 548 (VSB)

KYLE FEDOREK,

Defendant.

----------x

New York, N.Y.
February 19, 2015
10:10 a.m.

Before:

HON. VERNON S. BRODERICK,

District Judge

APPEARANCES

PREET BHARARA
United States Attorney for the
Southern District of New York
SARAH Y. LAI
Assistant United States Attorney

SERCARZ & RIOPELLE, LLP
Attorneys for Defendant
BY: MAURICE H. SERCARZ
JULIANA GRAHAM

ALSO PRESENT: NAVIN KALICHARAN, F.B.I.

Edgewater, New Jersey, if I have that right. A search ensued and a quantity of marijuana of over 25 pounds was confiscated as a result of the search. Apparently, there was a confidential informant among those that were in the apartment, and agents of law enforcement were following the car as it left the apartment.

A plea offer has been extended to a group of the defendants. The attorney understands it to be a global plea offer, meaning that the offer has been extended to the defendant on condition that everybody in the case accepts it. It calls for a sentence that in the vernacular in New Jersey is called five flat, which means in English that the defendant would be eligible for release after two years if he accepted the sentence.

To go on a little bit further, it is the defendant's intent and desire to plead guilty in connection with his participation in the events in New Jersey. And it is my hope that I can fashion a sentence for him that will allow him to do all of his time in custody in a federal facility and never have to endure either incarceration in a Bergen County facility or transportation from a federal jail to Bergen County for the purpose of a court appearance, then to waste away for a while in Bergen County, and then to be transported back to a federal facility with all of the attendant hardship.

What we are trying to accomplish with counsel in the

that we can give this Court that whatever term of incarceration he receives is going to provide adequate deterrence and that this Court need not be concerned that the defendant is going to go back out on the street when he's released and commit crimes other than this.

And if some kind of more objective evidence was required, then I commend to the Court the report from Daytop indicating his successful completion of the program and all of those pretrial services reports that demonstrate time after time after time negative urine samples.

Your Honor, all of these factors weigh in favor, I respectfully submit, of a shorter term of incarceration, the difficult term of incarceration that lies in store for Kyle, and then a maximum term of supervised release with requirements for drug treatment. I would urge the Court that if we have a genuine interest in making sure that the defendant is drug free, that he receives the education that he needs and the support that he needs to maintain a sober life and a productive life, the best way to do it is to get him out as soon as possible and to get him back into drug treatment. And it's for that reason that I recommended to the Court with the Jersey sentence in mind a period of incarceration of 24 months.

In conclusion, your Honor, notwithstanding that Kyle is 27 years old, I note that he was still living at home at the time of the offense and he's in many ways a very young man and

EXHIBIT 5

Ebldjohp
Plea

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

UNITED STATES OF AMERICA, New York, N.Y.

v. 14 Cr. 0404(JMF)

BRENDAN JOHNSTON,

Defendant.

----------x

November 21, 2014
10:08 a.m.

Before:

HON. JESSE M. FURMAN,

District Judge

APPEARANCES

PREET BHARARA
United States Attorney for the
Southern District of New York
BY: SARAH Y. LAI
Assistant United States Attorney

MICHAEL ZWEIBACK
Attorney for Defendant

- also present -

SA Patrick Hoffman, FBI

the proceeds of sales processed through the Blackshades' website. I never had access to the customer account information stored on the Blackshades servers.

On about October 20, 2011, I activated a Blackshades' account for a new customer and transmitted that information to the new customer by electronic message.

After I started working for Blackshades I learned through online posts that some of Blackshades' customers were using their remote access tool and other Blackshades' products for illicit purposes. For instance, some people would install a Blackshades' remote access tool onto computers without knowledge or consent of the computer owner. Once installed, the Blackshades user could use the tool to remotely control the other person's computer.

I also learned that Marjinz had caused the Blackshades' remote access tool to be programmed so Marjinz can control all of the computers onto which Blackshades' customers had installed it. Marjinz also had access to recover passwords and other information in all customer accounts on the Blackshades' server.

After learning how Marjinz was using the Blackshades' products, I continued working for Blackshades and posting and selling the product Blackshades for about 45 days. I worked for Blackshades until about September 2012.

I understand and agree that during my involvement with

THE COURT: All right. And when you did those things -- again, I recognize it sounds like at the beginning of this process you didn't necessarily understand the full scope of everything, but at some point when you did gain that knowledge and did the things that you described, did you know that what you were doing was wrong and against the law?

THE DEFENDANT: Yes.

THE COURT: All right. Mr. Szeiback, do you know of any valid defense that would prevail at trial or of any reason why Mr. Johnston should not be permitted to plead guilty?

MR. ZWEIBACK: No, your Honor.

THE COURT: Ms. Lai, are there any additional questions that you would like me to ask of Mr. Johnston?

MS. LAI: No, your Honor. Thank you.

THE COURT: And would you please summarize what the government's evidence would be if the defendant were to go to trial.

MS. LAI: Yes, your Honor.

If the case were to go to trial, the evidence that the government would present would include the following: Evidence from emails --

THE COURT: Could you just speak into the microphone as well, please?

MS. LAI: The government's evidence -- is that better?

THE COURT: I'm not sure your microphone is working,